Security

Risk level: High (not acceptable risk)

Ensure that all users with AWS Console access have Multi-Factor Authentication (MFA) enabled in order to secure your AWS environment and adhere to IAM security best practices.

This rule resolution is part of the Cloud Conformity Base Auditing Package

Audit

To determine if your IAM users are MFA-protected, perform the following:

Using AWS Console

Using AWS CLI

01 Sign in to the AWS Management Console.

02 Navigate to IAM dashboard at https://console.aws.amazon.com/ia

03 In the left navigation panel, select **Users**.

04 Click on the IAM user name that you want to examine.

05 On the IAM user configuration page, select **Security Credentials** tab.

06 Inside the **Sign-In Credentials** section, check the **Console password** and **Multi-Factor Authentication Device** status. If the **Console password** feature status is set to **Yes** and **Multi-Factor Authentication Device** is set to **No**, the

01 Run **list-users** command (OSX/Linux/UNIX) to list all IAM users within your account:

```
aws iam list-users
  --query 'Users[*].U
```

02 The command output should return an array that contains all your IAM user names:

```
[
    "John",
    "David",
    ...
    "Mark"
]
```

03 Run **get-login-profile** command (OSX/Linux/UNIX) to check if AWS Console access is enabled for the selected IAM user:

is not following AWS IAM security best practices.

07 Repeat steps no. 4 – 6 for each IAM user that you want to examine available in your AWS account.

04 The command output should return an object that contains the Login Profile for the selected IAM user:

```
{
    "LoginProfile": {
        "UserName": '
        "CreateDate":
        "PasswordRese
    }
}
```

If a **LoginProfile** object exists, then you should check if MFA is enabled below.

05 Run **list-mfa-devices** command (OSX/Linux/UNIX) to list the MFA devices (if any) for the selected IAM user:

```
aws iam list-mfa-devi
  --user-name John
```

MFA devices assigned to the specified IAM user:

```
{
    "MFADevices": []
}
```

If the **MFADevices** array returned for you is empty, i.e. **[ ]**, the selected IAM user authentication process is not MFA-protected.

07 Repeat steps no. 1 – 5 for each IAM user that you want to examine within your AWS account.

Remediation / Resolution

To enable MFA access protection for your IAM users, perform the following:

hardware) and their features visit http://aws.amazon.com/iam/details/mfa/

Using AWS Console

01 Sign in to the AWS Management Console.

02 Navigate to IAM dashboard at https://console.aws.amazon.com/ia

03 In the left navigation panel, select **Users**.

04 Click on the IAM user name that you want to update.

Using AWS CLI

01 Run **create-virtual-mfa-device** command (OSX/Linux/UNIX) to create a new virtual MFA device within your AWS account:

```
aws iam create-virtua
 --virtual-mfa-devic
 --outfile /root/QR
```

02 The command output should return the new virtual MFA device

dentials tab.

06 Inside the **Sign-In Credentials** section, click the **Manage MFA Device** button next to **Multi-Factor Authentication Device** to initiate the MFA device setup process.

07 In the **Manage MFA Device** dialog box, select **A virtual MFA device** and click **Next Step**.

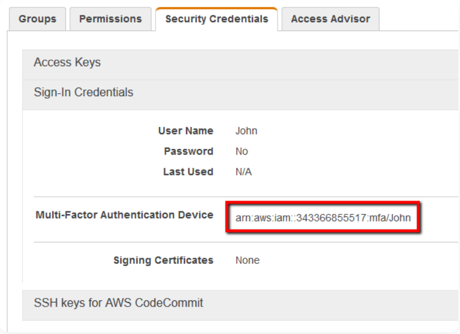
08 Now install the AWS MFA-compatible application. The MFA application used in this example is Google Authenticator. This guide assumes that you have already the application installed on your smartphone at this point, otherwise just follow these simple steps: https://support.google.com/account hl=en. Once the application is installed, click **Next Step**.

```
{
    "VirtualMFADevice
        "SerialNumber
    }
}
```

03 Run **enable-mfa-device** command (OSX/Linux/UNIX) to activate the specified MFA virtual device (in this case Google Authenticator) and associate it with the selected IAM user. The highlighted values represent two consecutive MFA device passcodes. The **enable-mfa-device** command is not returning an output:

```
aws iam enable-mfa-de
  --user-name John
  --serial-number arr
  --authentication-co
  --authentication-co
```

ication and enter two consecutive authentication codes in the **Authentication Code 1** and **Authentication Code 2** boxes, then click **Activate Virtual MFA** to complete the setup process. If successful, the following message will be displayed: **“The MFA device was successfully associated.”**. Click **Finish** to exit the setup wizard. The new MFA virtual device ARN should be listed inside the **Multi-Factor Authentication Device** section:



Access Keys

Sign-In Credentials

User Name John
Password No
Last Used N/A

Multi-Factor Authentication Device arn:aws:iam::343366855517:mfa/John

Signing Certificates None

SSH keys for AWS CodeCommit

10 Repeat steps no. 4 – 9 for all AWS IAM users

determine if the new MFA device has been successfully installed for the selected IAM user:

```
aws iam list-mfa-devi
  --user-name John
```

05 If successful, the command output should return the MFA device metadata (ARN, instantiation date, etc):

```
{
   "MFADevices": [
      {
         "UserName":
         "SerialNumbe
         "EnableDate'
      }
   ]
}
```

06 Repeat steps no. 1 – 5 for all AWS IAM users

References

AWS Documentation

AWS Identity and Access Management

FAQs

Multi-Factor Authentication

IAM Best Practices

Using Multi-Factor Authentication (MFA) in AWS

AWS Command Line Interface (CLI) Documentation

iam

list-users

list-mfa-devices

create-virtual-mfa-device

enable-mfa-device

AWS Blog(s)

Securing Access to AWS Using MFA--Part 1

Publication date May 21, 2016

- Pre-Heartbleed Server Certificates (Security)
- AWS IAM Access Keys Rotation (45 Days) (Security)
- SSL/TLS Certificate Renewal (30 days before expiration) (Security)
- IAM Password Expiry In 7 Days (Security)

Cloud Conformity allows you to automate the auditing process of *Enable MFA for AWS IAM Users*. **Register for a 14 day evaluation and check your compliance level for free!**

Check your compliance

Advanced
Technology
Partner

Security Competency

Cloud Management
Tools Competency